Chapter 20: Installing Kerberos on a non-Fermi-Supported Linux System

In this chapter we discuss Kerberizing a machine running a Linux OS other than FRHL, using the Fermi Kerberos source code from the MIT Kerberos product[1]. The instructions provided here should help non-UPS/UPD Linux users achieve a fully-functional Fermilab Kerberos implementation.

☞ The Computing Division does not support these types of installations explicitly, but you can request help on the *kerberos-users@fnal.gov* mailing list (and usually obtain it!).

20.1 Before You Install Kerberos

20.1.1 Obtain a Kerberos Principal

Strictly speaking, you don't need a Kerberos principal to just install the software. It will be difficult to judge your results without one, however. You'll need to get one (plus an initial password) to have access to the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal* for information. Use the online *Request Form for Computing Username and Primary Accounts* at `http://computing.fnal.gov/cd/forms/acctreq_form.html`.

20.1.2 Do you Need to Allow Incoming Kerberos Connections?

For any machine on which services will be offered and which therefore must allow incoming Kerberos connections (including portal mode connections) you must get a service principal for the host, and one for **FTP** if that is an offered service. These service principal names are of the form `host/<full.node.name>` and `ftp/<full.node.name>` (e.g.,

[1] Kerberos V5 is available from other sources as well, and these instructions should work for the general case, except of course for MIT-specific comments.

`host/mynode.fnal.gov` and `ftp/mynode.fnal.gov`, or something like `host/mynode.myuniv.edu` and `ftp/mynode.myuniv.edu`, depending on your institution's domain).

Before installing **kerberos** on a machine the first time, request these host-specific service principals (plus initial passwords) for that machine, using the form at `http://computing.fnal.gov/cd/forms/extra_kerb_req_form.html`. You will need to provide the full hostname of the machine.

☞ Notes:

- For a machine with two or more active (static) IP addresses or multiple node names, see section 16.12 *Multiple IP Addresses or Node Names*.
- If you are reinstalling **kerberos** on a machine, you should keep the same host and **FTP** principals. If the `krb5.keytab` is not lost, there's nothing you have to do for these principals. If it is lost, contact *compdiv@fnal.gov* to get password resets on the principals.

If you don't intend to allow incoming connections, don't request these service principals, and just answer "no" when asked if you have the passwords for them during installation of the **kerberos** product. You can request and install them at a later date, if needed (see section 16.10 *Installing Service Host Keys*).

20.1.3 Create an Account that Matches your Principal

We strongly recommend that you create an account/login name on the machine that matches the "primary" (the username part) of your user principal. See section C.2 *If your Principal and Login Name do not Match* under section Appendix C: *More about Choosing a Principal Name*. Note that even if your login name and principal don't match you can still get into your machine (console) after it's Kerberized, as long as your UNIX password is there.

20.1.4 Synchronize your Machine with Time Server

When using Kerberos, the client and server must be time-synchronized with each other, each in its local time zone. A wrong system clock is the single most common authentication problem (it typically appears as a "preauthentication failed" message). Kerberos is configured to allow a discrepancy of about five minutes. **xntp** is a product that you can install on your machine to maintain the system time in agreement with Internet standard time servers. It is available from *fnkits* for some platforms.

AFS

If your system runs AFS, don't install **xntp** or any other synchronizing software; AFS does its own synchronization. But beware: AFS doesn't set the hardware clock, so, for example, when daylight savings time starts or ends, your clock may be an hour off. Choose ONLY ONE of the following solutions:

- start **xntp**, let it sync the clock, then turn it off
- see if the **afsd** has a **`-nosettime`** option; if so, set it and run **xntp** to handle the timekeeping instead
- (Linux) make sure the date is correct, then run **`/sbin/hwclock --systohc`** to change the hardware clock to match the system clock (or edit your `crontab` to run the above command at some frequency; e.g., to sync it up once a month, add the line `33 3 3 * * /sbin/hwclock --systohc`)

20.2 Installing MIT Kerberos

1) Bring up the **MIT Kerberos** web page, at URL `web.mit.edu/kerberos/www/`. Select Kerberos V5, the latest release (this section was originally written for 1.2).

2) Follow the links to the MIT Kerberos Distribution page. You'll need to download the Kerberos source. Scroll down to Kerberos V5 Release 1.2 Source Distributions, and download (the latest; shown here for 1.2) `krb5-1.2.x.tar.gz, 5240k`.

3) Login as *root*.

4) Unzip and untar the file, creating the directory `krb5-1.2.x`

5) In the `krb5-1.2.x` directory, run `./configure` (use all defaults).

6) Still in `krb5-1.2.x`, run **`make`** and **`make install`**. Now, the software is configured, compiled and installed.

7) Get the latest `krb5.conf` file from Fermi KITS `ftp://ftp.fnal.gov:8021/KITS/GENERIC_UNIX/krb5conf/`. The `krb5.conf.template` file from the krb5conf product now has lines containing xMYREALMx and xMYNODEx which have to be edited. To join the production realm, change xMYREALMx to FNAL.GOV and xMYNODEx to the fully-qualified name of host. At this point, you should be able to authenticate to the Fermilab strengthened realm from your machine.

8) In the `/etc/inetd.conf` file, disable the default FTP, telnet,

rlogin[1], etc., on your machine, and enable the Kerberized versions. Also comment out or delete the lines starting with “shell”, “login”, “rexec” and insert new lines for kshell, klogin and eklogin:

```
## ftp  stream  tcp   nowait  root   /usr/local/sbin/ftpd    ftpd -a
ftp     stream  tcp   nowait  root   /usr/krb5/sbin/ftpd    ftpd -aOP
...
kshell  stream  tcp     nowait  root    /usr/krb5/sbin/kshd kshd -5c
klogin  stream  tcp     nowait  root    /usr/krb5/sbin/klogind klogind -5c
eklogin stream  tcp     nowait  root    /usr/krb5/sbin/klogind klogind -5ce
```

9) Run **`kadmin`**, and use **`ktadd`** to add host and FTP principals to the `/etc/krb5.keytab` file. Run **`kadmin`** as follows (supplying host and FTP passwords as needed):

```
% /usr/krb5/sbin/kadmin -p host/hostname.domain \

  -q “ktadd host/hostname.domain”

% /usr/krb5/sbin/kadmin -p ftp/hostname.domain \

  -q “ktadd ftp/hostname.domain”

kadmin: ktadd host/hostname.domain

kadmin: ktadd ftp/hostname.domain
```

At this point, you can FTP and telnet *into* your machine, as well as *from* it. Now, it’s time to replace the default login program with the Kerberized version. The typical RedHat login program is PAM-aware, but there is no PAM support in MIT Kerberos v1.2.2. In the RH Linux login file (`/etc/pam.d/login`) there is a line:

```
session    optional
  /lib/security/pam_console.so
```

The `pam_console.so` module is responsible for changing the ownership and permissions on the console devices. We recommend that you modify the source for the Kerberos `login.krb5` program, `krb5-1.2.x/src/appl/bsd/login.c`, to be PAM-aware.

10) To do this, **`cd`** to the the `krb5-1.2.x/src/appl/bsd/` directory, make a copy of `login.c` (to be safe!), copy the patch shown below into a file in this directory (we call it `patchfile`), and run it:

```
% patch -p0 < patchfile
```

Now the MIT Kerberos `login.c` will call the `pam_console.so` that came with RH Linux.

11) To link to the `pam` and `pam_misc` libraries, modify the Makefile in `krb5-1.2.2/src/appl/bsd`. Replace

[1] Note that klogind replaces rlogind, and kshd repalaces rshd.

```
LOGINLIBS =
```

with

```
LOGINLIBS = -lpam -lpam_misc
```

The Patch

```
--- login.c.origTue Mar  6 15:13:27 2001
+++ login.cWed Mar  7 15:44:56 2001
@@ -81,6 +81,10 @@

 #include <libpty.h>

+/* begin pam stuff */
+#include <security/pam_appl.h>
+#include <security/pam_misc.h>
+/* end pam stuff */
 #ifdef HAVE_UNISTD_H
 #include <unistd.h>
 #endif
@@ -1004,6 +1008,11 @@
     }
 }

+/* begin pam stuff */
+  int retcode;
+  pam_handle_t *pamh = NULL;
+  struct pam_conv conv = { misc_conv, NULL };
+/* end pam stuff */
 int main(argc, argv)
      int argc;
      char **argv;
@@ -1438,6 +1447,11 @@
     quietlog = access(HUSHLOGIN, F_OK) == 0;
     dolastlog(quietlog, tty);

+/* begin pam stuff */
+    retcode = pam_start("login.krb5", username, &conv,
&pamh);
+  pam_set_item(pamh, PAM_TTY, tty);
+  pam_open_session(pamh, PAM_SILENT);
+/* end pam stuff */
     if (!hflag && !rflag && !kflag && !Kflag && !eflag) {/*
XXX */
 static struct winsize win = { 0, 0, 0, 0 };
```

```
@@ -2394,6 +2408,10 @@
 #ifdef _IBMR2
     update_ref_count(-1);
 #endif
+/* begin pam stuff */
+   pam_close_session(pamh, PAM_SILENT);
+   pam_end(pamh, PAM_SUCCESS);
+/* end pam stuff */
```

This patch only enables the session module-type. If you add auth, account and/or password module-types, you may compromise the Kerberos security.

20.3 Installing Fermi Kerberos

20.3.1 Download Modified Source from CVS

Instead of installing non-Fermi Kerberos software and enabling the locally-added features of Kerberos, you can download the modified source from the Computing Division CVS repository:

```
% cvs -d :pserver:kpilot@cdcvs.fnal.gov:/cvs/cd co kerberos
```

Read (and be sure you understand!) the `README.*` files in the `ups/` directory. Then configure, compile and install.

20.3.2 Download Tar File from KITS

If you're running a Fermi-supported OS but not UPS/UPD, you can fetch the **kerberos** product tar file from fnkits.fnal.gov, untar it into `/usr/krb5`, then carry out the `/etc/services`, `/etc/inetd.conf` and `/etc/krb5.keytab` steps by hand, and get the `krb5.conf` file from the **krb5conf** product or from another system.

Assuming that you're logged on as *root* and `/usr/krb5/sbin` is in your PATH, the command to do the keytab file is:

```
kadmin -q "ktadd host/<node>.fnal.gov" -p host/<node>.fnal.gov

kadmin -q "ktadd ftp/<node>.fnal.gov" -p ftp/<node>.fnal.gov
```

and provide the passwords.